UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/037,800 | 01/04/2002 | Robert P. St. Pierre | 16159.035001; P6566 | 6933 |

32615 7590 03/13/2006

OSHA LIANG L.L.P./SUN
1221 MCKINNEY, SUITE 2800
HOUSTON, TX 77010

| EXAMINER | |
|---|---|
| GERGISO, TECHANE | |
| ART UNIT | PAPER NUMBER |
| 2137 | |

DATE MAILED: 03/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/037,800 | PIERRE ET AL. | |
| | Examiner | Art Unit | |
| | Techane J. Gergiso T-6 | 2137 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☐ Responsive to communication(s) filed on *08 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-3;15-27;2* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3;15-27;29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. This is a final office action response to the applicant's amendments filled on 12/08/2005.

2. The applicant amended independent claims 1, 15, and 29.

3. The applicant also canceled claim 14 and 28.

### *Response to argument.*

The applicant argues that Woodburn does not disclose creating and assigning a virtual address to a client process. The examiner disagrees with this matter because Woodburn and D. Mills (hereinafter "Woodburn") teach an Encapsulation that is responsible for mapping a given user space datagram to the encapsulation space. It would be clear to one skilled in the art that mapping a user space datagram involves the process of creating and assigning address. Woodburn also provides an Encapsulation architectural model in figure 1 of page 4. There is also further teaching of generation of encapsulation header described on figure 3 of page 6 by Woodburn. These are teaching evidences for creating and assigning a virtual address to a client.

The applicant also argues that "a user space as thought by Woodburn does not refer to a client but rather to a space in which a user resides". The examiner disagrees with this matter and believes that Woodburn teaching of a user space is inherently referring to a client. In addition, the user space as a host or client is indicated by Woodburn in figure 1 of page 4. Woodburn further teaches that it is possible to have a special encapsulation gateways with virtual interface on two virtual networks to form an entire virtual internet (Page 14: Last paragraph and Figure 4:

Virtual Networks Example) which; these virtual interface, virtual network and virtual internet described by Woodburn is also desired to be achieved by applicant described as Supernet, Channel and Virtual Address (see on specification, paragraph: 0005,0006,0007). Therefore, a user space as a client is well thought by Woodburn.

The applicant further argues that Woodburn does not disclose issuing a first IP version compliant packet, where the first IP version compliant packet comprises a security context, and where data in the first IP version compliant packet is encrypted using the security context. However, this is a newly amended claim and "where data in the first IP version compliant packet is encrypted using the security context" is not in the original disclosed claim filled on 01/04/2002. As far as the security is concerned, the examiner does not believe that wood burn does teach away. In fact is suggests that the authentication information be appended to the Encapsulated datagram. Woodburn continues to clarify on this by stating that information regarding the type of authentication or integrity check in use would have to be included in the flow management protocol which is used to distribute the flow information (Page 15: Section F: Security consideration). This flow protocol information is in accordance with IPv4 and IPv6 protocols defied in their header mapping. In case if IPv4 this is described on (Page 8: Table 1) under the field of security options and further suggests the use of authentication during generation of encapsulation header on (page 6: First Paragraph).

Applicant argues that Woodburn does not disclose prepending an issued packet with a second IP version header producing a second IP version compliant Packet, where the first IP

version is different than the second IP version. Again, this is a newly amended claim and "where the first IP version is different than the second IP version" is not in the original disclosed claim filled on 01/04/2002. However, Woodburn provides a 4bit version protocol to set the version number of the encapsulation protocol. (Page 10: A Packet Format; Figure 1: Encapsulation protocol header example). Further, Woodburn layouts the model architecture and suggests it is even possible to encapsulate many different OSI protocols within IP and IP within many other OSI protocols (Page 15: E. Encapsulation and OSI) let alone the invention claimed by the applicant as the encapsulation of one IP version in to the second IP version.

The applicant amended claims 1,15, and 29 by adding " *wherein data in the first Internet Protocol version compliant packet is encrypted using the security context*"; and "*wherein the first Internet Protocol version is different than the second Internet Protocol version*" and "decrypting and authenticating *data within* the stripped packet using a particular method as indicated by the security context producing a decrypted and authenticated Packet". The encapsulation of the first IP version in the second IP version is disclosed by Woodburn (Page 15: E. Encapsulation and OSI and (Page 10: A Packet Format; Figure 1: Encapsulation protocol header example). The security context to encrypt and decrypt data with in a packet is inherent with the IP vision used namely IP version 6. This security context is well disclosed in the IP version 6 specification. Further, Silvano in his book (IPV6: The New Protocol for Internet and Intranets), used as a second prior for this office action rejection, also teaches the encryption and decryption of data with the packet. This is described as a encrypted security payload (ESP) in section 8.1.3, page 156 Silvano.

Therefore, in view of the above, the examiner disagrees with applicants arguments and accordingly maintains the same rejections of the newly amended independent claims 1, 15, 29 and all directly or indirectly dependent claims.

***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claim 1-13, 15-27 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Woodburn in view of Silvano Gai (IPv6 The new Protocol for Internet and Intranet, published 12/12/97, http://www.IP.com)

As per claim 1:

Woodburn teaches in the RFC 1241of Internet Encapsulation Protocol that creating and assigning a virtual address to a client process (Page 2, Paragraph 9). The examiner interpreted

the user space defined by Woodburn as any client, either a physical host or a process node having physical or virtual address respectively (Figure 1; Page 13, Section D; Figure 4). Woodburn teaches issuing a first Internet Protocol version compliant packet, wherein the first Internet Protocol version compliant packet comprises a security context (Figure 1; Figure 2); prepending an issued packet with a second Internet Protocol version header producing a second Internet Protocol version compliant packet (Figure1; Figure 2; Page 4, Paragraph 3); and forwarding the second Internet Protocol version compliant packet to a recipient (Figure 1, Page 5,Paragraph 1).

Woodburn teaches also stripping away the second Internet Protocol version compliant header from the second Internet Protocol version compliant packet producing a stripped packet at the recipient (Page 9, Section 6; Figure 1);.

Woodburn suggests that to check the authentication or integrity of data, authentication information to be appended to the Encapsulation datagram (Page 15, Section F). Silvano, Oomori et al. in analogous art, however discloses in detail and explicitly that Authentication Header (AH) and Encrypted Security Payload (ESP) features if IPv6 is design to insure authenticity and integrity of IP packets (Section 8.1.1: Authentication Header; and Section 8.1.3: Encrypted Security Payload). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Woodburn to include the data in IPv6 is encrypted and decrypted using security context. This modification would have

been obvious because a person having ordinary skill in the art would have been motivated to do so, in order to improve the security issues of IPv4 as suggested by Silvano on ( page 151).

As per claim 2:

Woodburn does not explicitly teach that the first Internet Protocol is version 6. However, Silvano teaches that first Internet Protocol version compliant packet is Internet Protocol version 6 compliant packet (Page 230, Figure 2-12). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed by Woodburn that the first internet protocol is version 6. This modification would have been obvious because a person having ordinary skill in the art at the time of the invention was made, would have been motivated to do so since it is suggested by Woodburn (Page 15, Paragraph 2).

As per claim 3:

Woodburn does not explicitly teach that the second Internet Protocol is version 4. However, Silvano teaches that the second Internet Protocol version compliant packet is Internet Protocol version 4 compliant packet (Page 230, Figure 2-12). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed by Woodburn that the second internet protocol is version 4. This modification would have been obvious because a person having ordinary skill in the art at the time of the invention was made, would have been motivated to do so since it is suggested by Woodburn (Page 15, Paragraph 2).

As per claim 4:

Woodburn does not explicitly teach that the authentication server daemon. However, Silvano teaches the application of IPv6 security features applying AH and ESP using different ways (Page 160, Section 8.3) on the limitations of issuing the packet including executing a Supernet Attach Command with an authentication server daemon; responding to the Supernet Attach Command with a Supernet configuration information comprising the security context in the address; registering a mapping of the Supernet configuration information with a virtual address daemon. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed by Woodburn that issuing the packet to comprises daemon servers. This modification would have been obvious because a person having ordinary skill in the art at the time of the invention was made, would have been motivated to do so since it is suggested by Silvano (Figure 8, 9-13).

As per claims 5 and 19:

Woodburn does not explicitly teach that the security context address. However, Silvano teaches the application of IPv6 security features applying AH and ESP using different ways (Page 160, Section 8.3) addressing the limitations (virtual address, Supernet identity, and a channel identity). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed by Woodburn that the security context includes virtual address, Supernet identity, and a channel identity. This modification would have been obvious because a person having ordinary skill in the art at the time of the invention was made, would have been motivated to do so since it is suggested by Woodburn (Figure 4).

As per claims 6 and 20:

Neither Woodburn nor Silvano explicitly teach that the security context comprised of 128 bit unique value. However, using IPv6 packets, it is obvious and very well known to those skilled in the art that the claimed security context can be set to be comprised of a 128 bit unique value for an intended purpose as evidenced by similar bit setting in Silvano (Page 156, Figure 8-5).

As per claims 7 and 21:

Neither Woodburn nor Silvano explicitly teach that the security context comprised of a 16 bit set and a 112 bit set. However, using IPv6 packets, headers and addressing, it is obvious and very well known to those skilled in the art that the claimed bit partition to be comprised of a 16 bit set and a 112 bit set value for an intended purpose as evidenced by similar bit setting in Silvano (Page 154, Figure 8-1).

As per claims 8 and 22:

Neither Woodburn nor Silvano explicitly teach that 16 bit set denotes a site local Internet protocol address comprising 12 bits for an address prefix followed by 4 bits for a zero value. However it is obvious and very well known to those skilled in the art that denoting a 16 bit set to a site Internet protocol address comprising 12 bits for an address prefix followed by a b4 bit of a zero value for an intended purpose as evidenced by similar bit setting in Silvano (Page 156, Figure 8-5).

As per claims 9 and 23:

Neither Woodburn nor Silvano explicitly teach that the 112 bit set comprises contiguous bits for the Supernet identifier, the Channel identifier, and the virtual address. However, it is obvious and very well known to those skilled in the art that the 112 bit can be set to be contiguous and partitioned for the Supernet identifier, the Channel identifier, and the virtual address for the intended purpose as evidenced on the specification of the application itself (Page 8, Paragraph 0030) which this letter is addressing.

As per claims 10 and 24:

Neither Woodburn nor Silvano explicitly teach that 112 bit set comprises 64 bits Supernet identifier, 24 bits Channel identifier, and 24 bits virtual address. However, it is obvious and very well known to those skilled in the art that the 112 bit can be set to be partitioned to 64 bits Supernet identifier, 24 bits Channel identifier, and 24 bits virtual address for the intended purpose as evidenced on the specification of the application itself (Page 8, Paragraph 0030) which this letter is addressing.

As per claim 11:

Woodburn does not explicitly teach that the virtual address daemon maps virtual addresses. However, Silvano teaches the virtual address daemon maps the virtual address of the recipient process within the Supernet to an actual Internet protocol address (Figure 8-11). Therefore, it would have been obvious to a person in the art at the time the invention was made

to modify the method disclosed by Woodburn that the virtual address daemon maps virtual addresses. This modification would have been obvious because a person having ordinary skill in the art at the time of the invention was made, would have been motivated to do so since it is suggested by Woodburn (Page 4, Paragraph 3).

As per claims 12 and 26:

Neither Woodburn nor Silvano explicitly teach that the security context is encoded. However, it is obvious and very well known to those skilled in the art that the security context can be encoded according to a given standard format (encoding definition in American Heritage College dictionary).

As per claims 13 and 27:

The applicant of this application suggested that any packet management infrastructure may be used, appreciated by those skilled in the art, to obtain security context from the stripped packet using a handler mechanism (Page 9, Paragraph 0031). Therefore, it is obvious and very well known to those skilled in the art that the security context is obtained from the stripped packet using a handler mechanism.

As per claim 15:

Woodburn substantially teaches in the RFC 1241 of Internet Encapsulation Protocol that creating and assigning a virtual address to a client process (Page 2, Paragraph 9). The examiner interpreted the user space defined by Woodburn as any client, either a physical host or a process

node having physical or virtual address respectively (Figure 1; Page 13, Section D; Figure 4). Woodburn teaches issuing a first Internet Protocol version compliant packet, wherein the first Internet Protocol version compliant packet comprises a security context (Figure 1; Figure 2); prepending an issued packet with a second Internet Protocol version header producing a second Internet Protocol version compliant packet (Figure1; Figure 2; Page 4, Paragraph 3); and forwarding the second Internet Protocol version compliant packet to a recipient (Figure 1, Page 5,Paragraph 1).

Woodburn teaches also stripping away the second Internet Protocol version compliant header from the second Internet Protocol version compliant packet producing a stripped packet at the recipient (Page 9, Section 6; Figure 1);.

Woodburn suggests that to check the authentication or integrity of data, authentication information to be appended to the Encapsulation datagram (Page 15, Section F). Silvano, Oomori et al. in analogous art, however discloses in detail and explicitly that Authentication Header (AH) and Encrypted Security Payload (ESP) features if IPv6 is design to insure authenticity and integrity of IP packets (Section 8.1.1: Authentication Header; and Section 8.1.3: Encrypted Security Payload). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Woodburn to include the data in IPv6 is encrypted and decrypted using security context. This modification would have been obvious because a person having ordinary skill in the art would have been motivated

to do so, in order to improve the security issues of IPv4 as suggested by Silvano on ( page 151).

As Per claim 29:

Woodburn substantially teaches in the RFC 1241of Internet Encapsulation Protocol that the RFC 1241 provides a means or performing encapsulation in the Internet environment (Page 4 , Paragraph 1) and creating and assigning a virtual address to a client process (Page 2, Paragraph 9). The examiner interpreted the user space defined by Woodburn as any client, either a physical host or a process node having physical or virtual address respectively (Figure 1; Page 13, Section D; Figure 4). Woodburn teaches issuing a first Internet Protocol version compliant packet, wherein the first Internet Protocol version compliant packet comprises a security context (Figure 1; Figure 2); prepending an issued packet with a second Internet Protocol version header producing a second Internet Protocol version compliant packet (Figure1; Figure 2; Page 4, Paragraph 3); and forwarding the second Internet Protocol version compliant packet to a recipient (Figure 1, Page 5,Paragraph 1).

Woodburn teaches also stripping away the second Internet Protocol version compliant header from the second Internet Protocol version compliant packet producing a stripped packet at the recipient (Page 9, Section 6; Figure 1);.

Woodburn suggests that to check the authentication or integrity of data, authentication information to be appended to the Encapsulation datagram (Page 15,

Section F). Silvano, Oomori et al. in analogous art, however discloses in detail and explicitly that Authentication Header (AH) and Encrypted Security Payload (ESP) features if IPv6 is design to insure authenticity and integrity of IP packets (Section 8.1.1: Authentication Header; and Section 8.1.3: Encrypted Security Payload). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Woodburn to include the data in IPv6 is encrypted and decrypted using security context. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, in order to improve the security issues of IPv4 as suggested by Silvano on ( page 151).

### *Conclusion*

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

### *Contact Information*

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Techane J. Gergiso whose telephone number is (571) 272-3784. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

T. G

Techane Gergiso

Patent Examiner

Art Unit 2137

E. Moise

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

February 28, 2006